Cyber Security Awareness Month Tips for 2018

October is National Cyber Security Awareness Month. Given our reliance on mobile devices and the increasing number of web-connected devices we are welcoming into our homes, Wisconsin consumers are asked to use this month to consider ways to stay protected from cyber scam artists looking to steal their personal information and hard-earned money.

The Wisconsin Department of Agriculture, Trade and Consumer Protection (DATCP) recognizes this campaign by providing a cyber safety tip through our social media accounts each weekday in October. The 2018 tips are included in this document. Your organization can share these tips widely and reuse them throughout the year to help Wisconsin residents protect themselves online.

For additional information, visit the Wisconsin Bureau of Consumer Protection at http://datcp.wi.gov, send an email to datcphotline@wi.gov, or call the Consumer Protection Hotline at 800-422-7128. Connect with the Bureau on Facebook or Twitter.

Week 1: Simple Tips. Serious Protection.

Monday, 10/1. Take stock of your web-connected lifestyle

As we welcome additional web-enabled devices and applications into our lives, the line between our online and offline lives becomes less defined. We need to ensure that our accounts are secure so that we can use our devices with confidence.

The first step in strengthening the security around your devices and accounts is to take stock of these items in your home. Don't forget to include web-connected home devices as well, such as gaming devices, smartwatches, thermostats, smart TVs, routers, and voice assistants (Google Home, Amazon Alexa, etc.).

Once you have accounted for all of your devices (and your family members' devices), update the operating systems and antivirus software on the devices in order to protect against recent viruses and to patch any holes that hackers can use to access your systems.

Tuesday, 10/2. Keep an eye on your devices

Kind of a simple, self-explanatory tip today, but always keep your mobile devices with you in public and never leave them out "just for a minute." A couple of seconds is long enough for a thief to disappear with your device and your valuable data like contacts, messages, schedules, photos, music, mobile payment accounts and more.

Yesterday we suggested tracking down and updating all of your family's online devices. Now that they are accounted for, keep an eye on them in public and keep them locked up when not in use.

Wednesday, 10/3. Take active steps to protect your kids BEFORE they log on

Keep your home computer in a central location where you can monitor your children's online usage.

Look for any protection features (i.e. parental controls) that are built into the websites and software that your kids access and adjust them accordingly.

All major Internet service providers (ISPs) and cellular providers have tools to help you manage children's online experiences (e.g., selecting approved websites, monitoring the amount of time they spend online, limiting in-app purchases or limiting the people who can contact them).

For these tips and many more, visit the Raising Digital Citizens page at StaySafeOnline.org.

Thursday, 10/4. Think before you act

Ignore unsolicited emails, social media messages, phone calls or texts that create a sense of urgency and require you to respond immediately to a problem – particularly ones that supposedly involve your online account, bank account, taxes or package delivery. This type of message is likely a scam. When in doubt, don't respond.

If you question the legitimacy of a message that claims to be from a business or government agency, call the organization directly to inquire. Don't contact the organization on any phone number provided in the unsolicited call or voicemail and don't click any links in the email, social media post or text message.

Friday, 10/5. Saying goodbye to an old device? Don't say goodbye to your identity.

Looking to swap out for the latest smartphone? If you are trading in your phone at a retail store, the business will likely transfer your contacts to your new phone and wipe your data off your old phone. That's great. But what if you intend to donate, resell or recycle your old equipment?

Before you turn your old phone over to anyone or throw it in a donation bin, remember to completely erase your data and reset the phone to its initial factory settings. Check your device's general settings for a factory data reset option. If you don't know where to go, search online for information about your specific phone model or check with your cellular provider. Additional tips are covered on the Federal Trade Commission's (FTC) Disposing of Your Mobile Device webpage.

If you are getting rid of a desktop or laptop computer, you should make sure the hard drive is wiped completely clean before you let it go. The FTC's Disposing of Old Computers webpage includes considerations you need to make when disposing of a computer, including the importance of using specialized utility programs to wipe drives.

Monday, 10/8. Run a free computer security check, then build up your defenses

Start Week #2 with a clean sweep of your computer system. At the end of the month, sweep it again and make a plan to do so regularly.

StaySafeOnline.org has a list of free security check services.

Now that you know where you stand, build up your protections for the future. Make sure you have up-to-date antivirus and anti-spyware software and a firewall. Set this software to update its protections regularly. Install the latest security patches and bug fixes for your operating system and applications in order to protect against intrusions and infections that could compromise your computer files or passwords.

Tuesday, 10/9. Backup, backup, backup

A hard drive failure, device theft, or "ransomware" scam (a type of malware that locks up your files until you pay the scammer) could cost you all of your important documents and your photos, music, and videos. These things do happen and there is often little you can do to get your files back after the fact.

Don't let it happen to you. Backup your files fully and often.

Regularly sync your mobile devices with your laptop or desktop computer or to a cloud service. Backup your laptop or desktop to an external hard drive or cloud service. One misplaced mouse click or lost device could spell the end of all of your files…take steps NOW to protect your data.

Wednesday, 10/10. Run antivirus scans on external and USB flash drives

Did you know that viruses and malware can be transmitted via USB flash drives and other external devices? Use the security software on your computer to scan these devices before you access their contents. Plug in, run a scan, access files.

Thursday, 10/11. Think before you app

Malware lurks in downloadable applications. Only download software from authorized app stores – and even then, do some research about specific applications and developers before you make a purchase. Apps as simple and seemingly harmless as a flashlight utility have been found to harvest and send data to advertisers without informing the user.

Before downloading an application to your computer or mobile device, understand what information (your location, your contacts, access to social networks, etc.) the app accesses on your device. You can find this information within the app listing in the app store. For apps you have downloaded, each will have its own unique permissions that you can turn on/off within your device's main settings menu.

Friday, 10/12. Delete when done

Many of us download apps to our devices for specific purposes (such as planning a vacation or saving money at a particular business) and no longer need them after a while. Or we may have downloaded apps at some point that are no longer useful or interesting to us. Forgotten software that is not updated regularly could harbor vulnerabilities on your system. It's a good security practice to delete all apps you no longer use.

Monday, 10/15. Email and text message spam and scams

The terms “scam” and “spam” are almost interchangeable when it comes to email and text messages. Spam messages are junk bulk emails or texts that you receive without permission. The senders may be hocking “get rich quick” schemes and questionable products or they could be looking to get you to turn over personal or credit information (a practice known as “phishing” for data).

Did we mention that the messages can also transmit malware?

Simply put, if you get an odd email or text message out of the blue, delete it and take no further action. There is a lot to cover on email and text spam, so your best resource is DATCP’s “Spam” fact sheet.

Tuesday, 10/16. Microsoft is NOT calling. Watch for computer tech support scams

If you receive a call out of the blue claiming that your computer has a virus and that the caller can help you get rid of it, hang up immediately. It’s a scam. The callers often falsely claim to represent Microsoft or a local tech support company to gain the consumer’s trust. They tell the consumer that they can remove the (non-existent) virus from their computer for a fee. The caller asks the victim to download software from the internet that grants them remote access to the system.

If you allow these scammers to access your computer, they can load malicious software onto your machine and they may access your files as well. If you give them your credit card number to pay for their "services," they'll be happy to charge you despite doing nothing beneficial (and possibly causing harm) and they may add fake charges on your account.

This is typically a phone-based scam, but also shows up in online pop-up messages saying you have a computer virus and telling you to call them for help. Don't do it.

Wednesday, 10/17. That amazing, unbelievable online rental ad? Beware.

As always, if something seems too good to be true, it probably is. If you are looking online for a rental property and find an unreal deal, be very, very cautious.

Scammers steal information and pictures from real estate listings in order to post fraudulent apartment or home rental ads on Craigslist and other online sites. They may "rent out" a property that they don't own (or that doesn't even exist!) to multiple people, taking security deposits and first month's rents from all of these parties.

It's worth remembering that these types of fake classified ads are not only about rental properties – there are often fake ads for high-ticket items like cars, boats, and other vehicles. If a seller or a buyer refuses or is "unable" to meet for the transaction, by leery of the deal. If you are selling an item, turn away any buyer who sends you a check for way over your selling price and wants you to send back the difference (the check is fake and YOU will end up paying the bank back). If you are buying an item, watch out for requests to pay by wire transfer or pre-paid debit card…once your money is sent, it is nearly impossible to get it back if the ad is fake.

Craigslist offers these two simple tips: "Do not rent or purchase sight-unseen – that amazing 'deal' may not exist" and "Refuse background/credit checks until you have met landlord/employer in person."

Thursday, 10/18. Think before you post

Your fun-filled vacation photos could cause your grandma or grandpa to get scammed.

Why? Criminals can use the information you share on social media sites to create a narrative that they weave into their phony stories.

Consider the infamous "grandparent scam," where older citizens are called by a scammer claiming to be the person's grandchild. The "grandchild" claims to be on vacation, was in an accident or got arrested, and needs an immediate wire transfer to get out of the hospital or out of jail. Your social media account could provide a

tremendous amount of information for a scammer to use in their ploy, such as your name, family members' names, where you live and if you are away from home.

Remember those fun-filled pics I mentioned? By viewing your profile, the scammer knows you are away on vacation in ____ with your best friend ____. They can fill in the blanks, making for a much more believable con.

It's OK to share with friends and family on social media, but adjust the privacy settings for your accounts to block your content from strangers. Also, remember that sensitive information such as names, birth dates and Social Security numbers posted to social media accounts can be used by scammers to steal your identity. Keep private information private.

Friday, 10/19. Imposter scams

Many criminals are using government agency names or "look-alikes" in recent email and phone scams, hoping to add legitimacy to their ploys. Have you received an email from "State Court" about a required appearance? That's one (do NOT open the attachment in one of these emails!).

But it's not just government agencies whose identities are misused. Remember our tip on Tuesday regarding calls from fake tech support representatives looking for money for "repairs" and access to victims' computers? Those are imposter scams too, as are fake delivery confirmation emails that claim to come from legitimate shipping companies – these emails include a link or attachment that you are expected to click in order to learn about a supposed package delay or a problem with an order.

Don't fall for these ploys. Delete the emails and don't click any links. The fraudsters want your money, your personal information, or to infect your computer with malware. If you question the legitimacy of a communication from a business or governmental agency, contact DATCP's Consumer Protection Hotline (800-422-7128) or call the misrepresented agency directly to inquire (but don't use the phone number that was provided in the questionable message!).

For more tips, check out DATCP's "Imposter Scams" fact sheet.

Monday, 10/22. Mobile device passwords

Most smartphones and tablets require users to enter passcodes to access the device. It may be a minor inconvenience, but it's tough to argue how valuable that extra security step is…our mobile devices carry an incredible amount of information. Cyber thieves know this and will do anything to get at that data.

Use a unique passcode for each device. For added security, use the device's fingerprint reader for unlocks.

Tuesday, 10/23. Lost phone? Bad. Lost data? Worse.

If your smartphone or tablet is lost or stolen, you want to have a fighting chance at finding it or at least at wiping out any personal data before it's accessed by the wrong party. For this purpose, there are tracking applications available for the major mobile device operating systems.

If you are a Google Android user, your device uses a "Find My Device" feature (available on the Google Play Store). On Apple devices, look for "Find My iPhone" in the Settings menu.

Using these tools, you can remotely locate your device or lock or erase your device, but you need to make sure the features are active and properly set up before you run into trouble.

Wednesday, 10/24. Use caution on public networks

If you are using a public Wi-Fi hotspot to connect to your personal accounts on a mobile device, limit the types of business you conduct, shield your typing from prying eyes, and set your device to hide your password character entries. Hold off on using online banking websites or sites that require personal information (like Social Security numbers) until you are on a secure private network or a home computer.

Be aware that there are "imposter" hotspots out there – Wi-Fi networks run by scammers that are made to appear like they are provided by a local business. The actions you take on an impostor network are visible to the person running the network. Again, limit the types of actions you take on any public network to minimize your risk of unknowingly sharing information with crooks.

BONUS TIP: on any web browser (mobile or desktop/laptop alike), look to see if the website encrypts the information it transmits BEFORE you enter and submit any personal information like passwords, security questions, banking information, etc. How can you tell if a site is encrypted? Check that the URL (the web address) starts with "https" rather than "http." The "s" stands for "secure." Easy, right?

Thursday, 10/25. Watch for data hungry apps

Every time you download a new application, check the data usage settings in the device settings menu to ensure that the app will not drain your data behind the scenes. Even programs that have solid ratings in the app stores may run data-intensive processing in the background. You may not realize that this is occurring until your service provider warns you that you're running low on available data for the month – depending on your service plan, this could end up costing you an additional payment for more data or could lead to your data speeds being throttled for the rest of the month.

Friday, 10/26. Tag, you're it! And in trouble.

"Geotagging," or linking GPS coordinates with your photos and online posts, is often turned on as a preset on mobile devices. Be very careful how you utilize this feature – this data could be used by criminals to target you in a scam or ID theft operation.

Pay attention to which applications use location-based features in your device and app settings.

Week 5: Lock Down Your Login

Monday, 10/29. Build better passwords, be better protected

Take steps to strengthen the security around your online accounts by creating longer, more complex passwords that are tougher to crack. Use a passphrase: a combination of numbers, letters, and special characters that spells out a phrase that you will remember.

For example, the phrase "I am happy to be here!" could be coded as "Iam:)2bH!"

Keep unique passwords for every online account and make sure to use an especially strong password for your email. Many websites send password update and account access emails to users, so getting a hold of these emails could potentially give a hacker access to all of your online accounts. Your email password should be the toughest to decode.

For more tips, check out DATCP's "Creating Strong Passwords" fact sheet.

Tuesday, 10/30. Use two-factor authentication when available

Two-factor authentication is a security process in which you provide two means of identification in order to log into a system – something you have and something you know. Something you have is typically a physical token, such as a fob, fingerprint, or a code sent to your smartphone. Something you know is something memorized, such as a personal identification number (PIN) or a password.

If it sounds confusing, think about this: when you use your credit card at the gas pump, you already use two-factor authentication. You swipe your card (something you have) and enter your ZIP code (something you know). So if one of your favorite websites strengthens its security features and offers to send you an additional passcode for logging in, take them up on it.

Wednesday, 10/31. Your educational journey awaits!

October may be coming to an end, but your cyber education is just beginning! There are a number of great resources available to help you strengthen the security around your web-enabled devices and online accounts.

Start with the DATCP website (datcp.wi.gov), particularly our consumer protection fact sheets, identity theft fact sheets, and Consumer Alerts. Remember to contact the Consumer Protection Hotline (800-422-7182; datcphotline@wi.gov) if you ever question a sales pitch or a threat you receive by email, text, or phone.

The National Cyber Security Alliance's StaySafeOnline website (staysafeonline.org) offers a wealth of cyber tips for families and businesses alike.

The FTC's Consumer Blog (consumer.ftc.gov) offers near-daily posts about scams that Americans are facing and actions the agency is taking against fraudsters. Keeping abreast of the latest scams will help you stay ahead of the con artists.

The FBI has developed a free computer literacy program called "Safe Online Surfing" or "SOS." SOS is a series of online games for grades three through eight that help your child learn about important cyber security topics like passwords, downloading apps, screening friend requests and more. Check it out at sos.fbi.gov.